UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/855,808	05/15/2001	Gerald R. Malan	UOM0234PUS	1533

7590 05/05/2005

David R. Syrowik
Brooks & Kushman P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1351

EXAMINER	
FIELDS, COURTNEY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/855,808	MALAN ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 February 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The Examiner has accepted changes made to the claims.

Response to Arguments

2. Applicant's arguments filed 11 February 2005 have been fully considered but they are not persuasive.

3. Referring to the rejection of claim 1, the Applicant contends and argues that the prior art Belissent (US Patent 6,789,203) does not disclose a collector adapted to receive such statistics from a routing system of a computer network as only provided by the present invention. The Examiner respectfully disagrees and asserts that Belissent does teach a collector (throttler unit) is capable of receiving data packet flow information routed from a network. A data packet flow statistic is considered by the throttler unit. (See Column 5, lines 36-56)

4. Referring to the rejection of claim 1, the Applicant contends and argues that the prior art Belissent (US Patent 6,789,203) does not disclose detecting one or more data packet flow anomalies to generate a signal nor disclose tracking attributes related to one or more data packet flow anomalies to a source. The Examiner disagrees and asserts that however, Belissent does teach a throttler unit as means for detecting data packet flow anomalies once a request rate has been exceeded (i.e. anomalies) the processing unit directs the throttler unit to prevent any further acceptance of connection requests from the offending requestor. This method allows the throttler unit to determine the offending requestor (i.e. source). The client's unique IP address (i.e. tracking

attributes) is used by the throttler as a means for identifying and preventing any denial of service attacks. (See Column 5, lines 36-67, Column 6, lines 1-17)

5. Therefore, the rejection of claims 1-33 are maintained in view of the reasons above and in view of the reasons below.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Belissent (US Patent No. 6,789,203).

Regarding claim 1, Belissent teaches a system for detecting, tracking and blocking one or more denial of service attacks over a computer network, the system comprising:

a collector adapted to receive a plurality of data statistics from the computer network and to process the plurality of data statistics to detect one or more data packet flow anomalies and to generate a signal representing the one or more data packet flow anomalies (col.5 lines 45-56), and

a controller coupled to the collector to receive the signal (col.6 lines 2-17: throttler unit 216) ;

wherein the controller is constructed and arranged to respond to the signal by tracking attributes related to the one or more data packet flow anomalies to at least one source, and wherein the controller is constructed and arranged to block the one or more data packet flow anomalies (col.6 lines 2-17: throttler unit 216).

Regarding claim 2, Belissent teaches the collector includes a buffer coupled to the computer network and being adapted to process the plurality of data statistics to generate at least one record (col.5 lines 36-51).

Regarding claim 3, Belissent teaches the collector further includes a profiler coupled to the buffer and being adapted to receive and process the record to generate a predetermined threshold (col.5 line 48 thru col.6 line 17).

Regarding claim 4, Belissent teaches the profiler includes means for aggregating the data statistics to obtain a traffic profile of network flows (col.5 line 48 thru col.6 line 17).

Regarding claim 5, Belissent teaches the data statistics are aggregated base on at least one invariant feature of the network flows (col.5 line 48 thru col.6 line 17).

Regarding claim 6, Belissent teaches data statistics are aggregated based on temporal, statistic network and dynamic routing parameters (col.5 line 48 thru col.6 line 17).

Regarding claim 7, Belissent teaches the at least one invariant feature includes source and destination endpoints (col.5 line 48 thru col.6 line 17).

Regarding claim 8, Belissent teaches the collector further includes a detector coupled to the buffer and to the profiler, the collector being adapted to receive and

process the record and the predetermined threshold to detect if attributes associated with the record exceed the predetermined threshold representing the one or more data packet flow anomalies (col.5 line 48 thru col.6 line 17).

Regarding claim 9, Belissent teaches the collector further includes a local controller coupled to the detector and to the profiler and being adapted to receive and respond to the one or more data packet flow anomalies by generating the signal representing the one or more data packet flow anomalies (col.5 line 48 thru col.6 line 17).

Regarding claim 10, Belissent teaches the detector includes a database for storing the at least one record, predetermined threshold, the one or more data packet flow anomalies, and related information (col.5 lines 56-61).

Regarding claim 11, Belissent teaches the profiler includes a database for storing a plurality of data packet flow profiles and related information (col.5 lines 56-61).

Regarding claim 12, Belissent teaches the controller includes a filtering mechanism for blocking the one or more data packet flow anomalies (col.5 line 48 thru col.6 line 17, col.6 lines 26-40).

Regarding claim 13, Belissent teaches the filtering mechanism includes a plurality of filter list entries (co1.5 line 48 thru col.6 line 17, co1.6 lines 26-40).

Regarding claim 14, Belissent teaches the filtering mechanism includes a plurality of rate limiting entries (col.5 line 48 thru col.6 line 17-, col.6 lines 26-40).

Regarding claim 15, Belissent teaches the controller includes a correlator coupled to the collector and being adapted to receive and normalize the plurality of

signals representing the one or more data packet flow anomalies and to generate an anomaly table including the attributes related to the one or more data packet flow anomalies (col.5 line 48 thru col.6 line 17; col.6 lines 41-44).

Regarding claim 16, Belissent teaches the correlator includes a database for storing the anomaly table (col.5 lines 56-61, col.6 lines 41-44).

Regarding claim 17, Belissent teaches the correlator further includes an adapter that is constructed and arranged to communicate the anomaly table to a computing device for further processing (col.5 lines 56-61).

Regarding claim 18, Belissent teaches the controller further includes. :

a web server (col.5 lines 6-9), and

access scripts that cooperate with the web server to enable the access the database defined on the controller to view the computing device to anomaly table (col.5 line 56 thru col.6 line 17).

Regarding claim 19, Belissent teaches a system comprising:

at least one routing system (col.5 lines 42-56),

a plurality of computer systems coupled to the routing system, and means for detecting one or more denial of service attacks communicated to the plurality of computer systems over the at least one routing system (col.1 lines 46-51, col.5 lines 4-9, col.5 line 48 thru col.6 line 17.

Regarding claim 20, Belissent teaches a means for tracking the one or more denial of service attacks communicated to the plurality of computer systems over the at least one routing system (col.5 line 34 thru col.6 line 17).

Regarding claim 21, Belissent teaches a means for blocking the öne or more denial of service attacks communicated to the plurality of computer systems over the at least one routing system (col.5 line 34 thru col.6 line 17).

Regarding claim 22, Belissent teaches means for detecting includes a means for collecting a plurality of data statistics from the at least one routing system (col.5 line 34 thru col.6 line 17).

Regarding claim 23, Belissent teaches the means for detecting further includes a means for processing the plurality of data statistics to detect one or more data packet flow anomalies (col.5 line 34 thru col.6 line 17).

Regarding claim 24, Belissent teaches the means for detecting further includes a means of generating a plurality of signals representing the one or more data packet flow anomalies (col.5 line 34 thru col.6 line 17).

Regarding claim 25, Belissent teaches the means for tracking includes a means for receiving and responding to the plurality of signals by tracking attributes related to the one or more data packet flow anomalies to at least one source (col.5 line 34 thru col.6 line 17).

Regarding claim 26, Belissent teaches a means for communicating the one or more denial of service attacks to a computing device for further processing (co1.5 line 34 thru col.6 line 17).

Regarding claim 27, Belissent teaches a method for detecting, tracking and blocking one or more denial of service attacks over a computer network, the system comprising the steps of:

collecting a plurality of data statistics from the computer network;

processing the plurality of data statistics to detect one or more data packet flow anomalies,

generating a plurality of signals representing the one or more data packet flow anomalies, and

receiving and responding to the plurality of signals by tracking attributes related to the one or more data packet flow anomalies to at least one source (col.5 line 34 thru col.6 line 17).

Regarding claim 28, Belissent teaches the step of blocking the one or more data packet flow anomalies in close proximity to the at least one source (col.5 line 34 thru col.6 line 17).

Regarding claim 29, Belissent teaches the step of collecting the plurality of data statistics includes:

buffering the plurality of data statistics',

processing the plurality of data statistics to generate at least one record', and

receiving and profiling the at least one record to generate a predetermined threshold (col.5 line 34 thru col.6 line 17).

Regarding claim 30, Belissent teaches the step of collecting the plurality of data statistics further includes:

detecting if attributes related to the at least one record exceed the predetermined threshold representing the one or more data packet flow anomalies (col.5 line 34 thru col.6 line 17).

Regarding claim 31, Belissent teaches the step of collecting the plurality of data statistics further includes:

responding locally to the one or more data packet flow anomalies by generating the plurality of signals representing the one or more data packet flow anomalies (col.5 line 34 thru col.6 line 17).

Regarding claim 32, Belissent teaches the step of receiving and responding to the plurality of signals includes:

correlating the plurality of signals representing the one or more data packet flow anomalies, and

generating an anomaly table including the attributes related to the one or more data packet flow anomalies (col.5 line 34 thru col.6 line 17).

Regarding claim 33, Belissent teaches the step of receiving and responding to the plurality of signals further includes the step of communicating the anomaly table to a computing device for further processing (col.5 line 34 thru col.6 line 17).

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cdf
April 27, 2005

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137